



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11187013 A**

(43) Date of publication of application: 09 . 07 . 99

(51) Int. Cl.

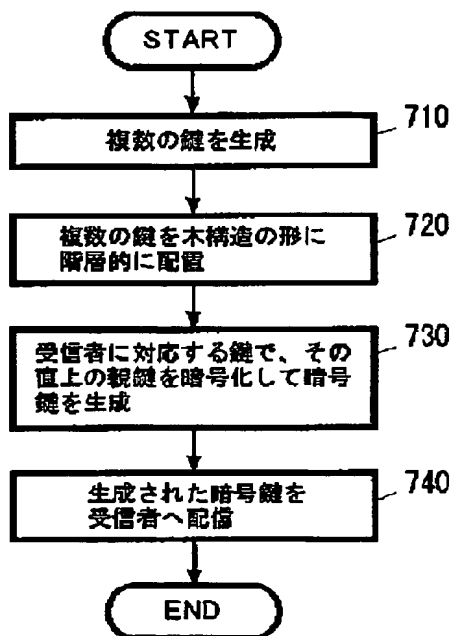
**H04L 9/08
G09C 1/00**(21) Application number: **09354401**(22) Date of filing: **24 . 12 . 97**(71) Applicant: **IBM JAPAN LTD**(72) Inventor: **MARUYAMA HIROSHI
TOKUYAMA TAKESHI
URAMOTO NAOHIKO**(54) **CRYPTOGRAPHIC KEY DISTRIBUTION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method and a system for minimizing procedures required for updating a cryptographic key by structuring the cryptographic key into tree structure.

SOLUTION: First of all, plural keys more than the number of recipients are generated 710, and the plural keys are hierarchically arranged 720 in the form of tree structure. Next, the plural recipients are made correspondent to the keys hierarchically arranged in the form of tree structure, and the cryptographic keys of the respective recipients are generated as a key stream having keys from the root of tree structure to positions corresponding to the said recipients in the tree structure. Thus, after the cryptographic key is generated 730, the generated cryptographic key is distributed 740 to the correspondent recipient.

COPYRIGHT: (C)1999,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-187013

(43) 公開日 平成11年(1999) 7月9日

(51) Int.Cl.⁵

H 0 4 L 9/08

G 0 9 C 1/00

識別記号

6 3 0

F I

H 0 4 L 9/00

G 0 9 C 1/00

H 0 4 L 9/00

6 0 1 B

6 3 0 B

6 3 0 D

6 0 1 D

審査請求 未請求 請求項の数11 O L (全 6 頁)

(21) 出願番号 特願平9-354401

(22) 出願日 平成9年(1997)12月24日

(71) 出願人 592073101

日本アイ・ピー・エム株式会社

東京都港区六本木3丁目2番12号

(72) 発明者 丸山 宏

神奈川県大和市下鶴間1623番地14 日本ア

イ・ピー・エム株式会社東京基礎研究所内

(72) 発明者 徳山 豪

神奈川県大和市下鶴間1623番地14 日本ア

イ・ピー・エム株式会社東京基礎研究所内

(72) 発明者 浦本 直彦

神奈川県大和市下鶴間1623番地14 日本ア

イ・ピー・エム株式会社東京基礎研究所内

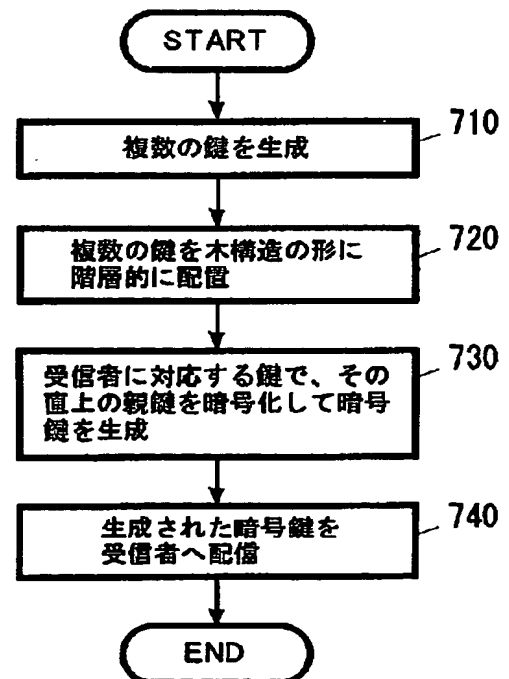
(74) 代理人 弁理士 坂口 博 (外1名)

(54) 【発明の名称】 暗号鍵配信システム

(57) 【要約】

【課題】暗号鍵を木構造に構造化することで、暗号鍵更新のための手間を最小にする方法及びシステムを提供することである。

【解決手段】上記課題を解決するために、まず受信者の数以上の、複数の鍵を生成し、複数の鍵を、木構造の形に階層的に配置する。次に複数の受信者を木構造の形に階層的に配置された鍵と対応付け、受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する。このようにして暗号鍵を生成した後、生成された暗号鍵を、対応する前記受信者へ配信する。



【特許請求の範囲】

【請求項1】複数の受信者に配信するための暗号鍵を生成する、暗号鍵生成システムであって、(a)前記受信者の数以上の、複数の鍵を生成する手段と、(b)前記複数の鍵を、木構造の形に階層的に配置する手段と、

(c)前記複数の受信者を前記木構造の形に階層的に配置された鍵と対応付け、前記受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する手段と、を具備することを特徴とする、暗号鍵生成システム。

【請求項2】暗号鍵を複数の受信者へ配信する、暗号鍵配信システムであって、(a)前記受信者の数以上の、複数の鍵を生成する手段と、(b)前記複数の鍵を、木構造の形に階層的に配置する手段と、(c)前記複数の受信者を前記木構造の形に階層的に配置された鍵と対応付け、前記受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する手段と、(d)生成された暗号鍵列を、対応する前記受信者へ配信する手段と、を具備することを特徴とする、暗号鍵配信システム。

【請求項3】前記暗号鍵を配信する手段(d)が、対応する前記受信者の公開鍵を用いて暗号化した後、配信する手段である、請求項2記載のシステム。

【請求項4】前記暗号鍵を配信する手段(d)が、インターネットを通じて配信する手段である、請求項2記載のシステム。

【請求項5】前記暗号鍵を配信する手段(d)が、衛星放送を通じて配信する手段である、請求項2記載のシステム。

【請求項6】前記木構造が2進木、3進木、若しくは4進木である、請求項1乃至2の何れかに記載のシステム。

【請求項7】前記複数の受信者の中から、脱退者がした場合、前記複数の鍵の内、該脱退者が有する暗号鍵に関連する鍵のみを変更して、該鍵の直下の鍵で暗号化して、受信者に変更された暗号鍵を、配信する手段を具備する、請求項2記載のシステム。

【請求項8】前記暗号鍵を生成する手段(c)が、前記複数の受信者を、予め受信者の属性によりグループ分けを行い、グループ間の関係に従い、前記複数の受信者を前記木構造の形に階層的に配置された鍵と対応付ける手段を含む、請求項1乃至2の何れかに記載のシステム。

【請求項9】前記属性が受信者の、契約年数、加入時期、年齢、職業、住所、会社、若しくは電話番号である、請求項8記載のシステム。

【請求項10】複数の受信者に配信するための暗号鍵を生成する、暗号鍵生成方法であって、(a)前記受信者の数以上の、複数の鍵を生成する段階と、(b)前記複数の鍵を、木構造の形に階層的に配置する段階と、

(c)前記複数の受信者を前記木構造の形に階層的に配置された鍵と対応付け、前記受信者の個々の暗号鍵を、

木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する段階と、を有することを特徴とする、暗号鍵生成方法。

【請求項11】複数の受信者に配信する暗号鍵を生成するためのプログラムを含む媒体であって、該プログラムが、(a)前記受信者の数以上の、複数の鍵を生成する機能と、(b)前記複数の鍵を、木構造の形に階層的に配置する機能と、(c)前記複数の受信者を前記木構造の形に階層的に配置された鍵と対応付け、前記受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する機能と、

を有することを特徴とする、プログラムを含む媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本願は、衛星放送あるいはインターネットにおけるマルチキャストのような放送型メディアにおける、暗号鍵配信システムに関し、特に鍵を木構造に構造化することで、暗号鍵更新のための手間を最小にする方法およびシステムに関する。

【0002】

【従来の技術】衛星放送あるいは、インターネットにおけるマルチキャストのような放送型メディアにおいて、ユーザーの認証及びデータの暗号化を行う場合、受信者(subscriber)に鍵の配信を行わなければならない。新たに受信者が参加する場合には、その人に現在使っている鍵を渡せば良いが、受信者が参加をやめた場合、データの暗号鍵を更新する必要がある。

【0003】例えば受信者(subscriber)の集合をSとする。Sは特定の有料番組を視聴している視聴者と仮定する。あるいは、企業内である機密の連絡を待っている従業員の集合でもよいし、インターネット上でよく使われているメイリングリストの、参加者の集合をSとしてもよい。

【0004】Sにはn人の受信者がいるとする。図1では、アリスとボブとキャロルはSの要素である。放送者(publisher)PはコンテンツCを、暗号化して送り出す。インターネットの世界では、標準化団体IETFが、メイリングリストの暗号化の標準化案として、RFC1421を提案している。これは、共通のセッション鍵KでメッセージMを暗号化し(K(M))、さらにそのKをn人の個々の暗号化鍵D1...Dnで暗号化し(D1(K), D2(K), ..., Dn(K))、それをK(M)とともに、送り出すというものである(図2参照)。受信者は対応する復号化鍵(E1, E2, ..., En)でセッション鍵Kを復号化し、得られたKでメッセージMを復号化する。この方式はしかし、受信者の数nが大きくなると、メッセージに比して鍵パケットの大きさが非常に大きくなってしまいうという欠点がある。例えば個人鍵に512ビットのRSA鍵を用いた場合、一つのDi(K)は最低64バイトになり、nが例えば10,000だと一つのメッセージ

につき、640KBytesの鍵パケットを送り出さなければならない。

【0005】共通のセッション鍵Kをあらかじめ各受信者の個人鍵を使って配布しておく方法(Join/Leave Mode 1)を考えた場合を図3に示す。個人鍵は、一般的な公開鍵証明書に基づくものでよいし、アプリケーション毎に用意されたものであってもよい。ここで問題となるのは、受信者の集合Sに変更があった場合である。すなわち、Sに新たな要素が加わった場合、つまり新しい視聴者が参加した場合などは、そのユーザーの身元を個人鍵を使って認証し、Kを配れば良いが、Sの要素がSから抜けた場合には、鍵の更新が大変である。例えば、キャロルが支払日になっても視聴料を支払わなかったために、Sから除こうとしたとする。彼女はKを持っているために、同じセッション鍵を使い続けるわけにはいかない。単純には、新しい鍵K'を生成し、それを残ったn-1人の受信者にそれぞれの個人鍵を使って送らなければならない。これでは、nが大きい場合、例えば10万人の視聴者がいる場合、一人が抜ける度に10万の鍵配送が起きてしまうことになる。

【0006】従来、有料衛星通信などに現在使われている技術は、秘密アルゴリズム方式で各社の方式に互換性がなく、また、デコーダの所有が鍵の所有となっているので、ダイナミックに新たな視聴者を参加させたり一時的に脱退させたりすることができない。例えばペイパービューなどで使われている方式は、鍵の配送を電話による1対1の通信に頼っており、上り回線を必要とすること、スケールしないこと、などの問題点がある。

【0007】その他、インターネットでのマルチキャストのセキュリティとして、ルータからグループ鍵を配信する方法が提案されている。しかし、この方式では、信頼できるルータをネットワーク上にあらかじめインストールしておかなければならない、という重大なセキュリティ上の問題がある。また、この方式は、IPのレイヤーでのセキュリティであり、アプリケーションからのエンドツーエンドのセキュリティを保証するものではない。

【0008】

【発明が解決しようとする課題】従って、本発明が解決しようとする課題は、暗号鍵を木構造に構造化することで、暗号鍵更新のための手間を最小にする方法及びシステムを提供することである。また別の課題は、既知の暗号技術の上で動くために規格を公開できる、暗号鍵配信の方法及びシステムを提供することである。また別の課題は、各社の相互接続性が保ち、上り回線を使うことのない、動的な視聴者の参加及び脱退が可能な、暗号鍵配信の方法及びシステムを提供することである。また別の課題は、通信途中にいくらセキュリティ上の問題がある経路があっても全体のセキュリティは保つことのできる、暗号鍵配信の方法及びシステムを提供することである。

【0009】

【課題を解決するための手段】上記課題を解決するために、まず受信者の数以上の、複数の鍵を生成し、複数の鍵を、木構造の形に階層的に配置する。次に複数の受信者を木構造の形に階層的に配置された鍵と対応付け、受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する。このようにして暗号鍵を生成した後、生成された暗号鍵を、対応する前記受信者へ配信する。なお木構造では、根(ルート)から派生する各枝から、さらに派生する枝を有する。本発明の方法では、その派生する枝の数に限定はない。つまり根から派生する枝が2であり、その各枝から派生する枝が3であっても構わない。逆にn進木のように一定でもよい。図4(2進木の形の場合)では、木のルートにあるK0がセッション鍵である。コンテンツはこのセッション鍵で暗号化される。K0は、K1、K2でそれぞれ暗号化されて受信者に配信される。これをK1(K0)、K2(K0)と略記する。同様に、鍵K1はK3とK4で暗号化され、配信される。なお鍵の配信は、各個人の公開鍵で暗号化して送ってもよい。セキュリティ上安全であれば、各個人の公開鍵で暗号化して送る必要はない(例えばディスクットによる手渡しでも構わない)。また配信手段として、インターネットを通じて配信してもよいし、衛星放送を通じて配信してもよい。その他、本発明の本質に拘らず、適宜変更可能である。このように構成することにより、暗号鍵更新のための手間を最小にすることができる。

【0010】

【発明の実施の形態】図6に、本発明の暗号鍵生成システムのブロック図を示す。まずブロック610で、受信者の数以上の、複数の鍵を生成する。次にブロック620で、複数の鍵を木構造の形に階層的に配置する。最後にブロック630において、複数の受信者を木構造の形に階層的に配置された鍵と対応付け、受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する。

【0011】図7に、本発明の暗号鍵配信システムのブロック図を示す。基本的に暗号鍵生成システムと同様であるが、まずブロック710で、受信者の数以上の、複数の鍵を生成する。次にブロック720で、複数の鍵を木構造の形に階層的に配置する。次にブロック730で、複数の受信者を木構造の形に階層的に配置された鍵と対応付け、受信者の個々の暗号鍵を、木構造の根から、木構造の該受信者に対応付けられた位置に至る鍵を有する、鍵列として生成する。そして最後にブロック740において、生成された暗号鍵を対応する受信者へ配信する。

【0012】

【実施例】以下、図面を参照して本発明の実施例を説明する。図8には、本発明において使用される暗号鍵配信

システムのハードウェア構成の一実施例を示す概観図が示されている。特にインターネットを通じて暗号鍵を配信するシステムの典型的例である。システム100は、中央処理装置(CPU)1とメモリ4とを含んでいる。CPU1とメモリ4は、バス2を介して、補助記憶装置としてのハードディスク装置13(またはMO、CD-ROM23、DVD等の記憶媒体駆動装置)とIDEコントローラ25を介して接続してある。同様にCPU1とメモリ4は、バス2を介して、補助記憶装置としてのハードディスク装置30(またはMO28、CD-ROM23、DVD等の記憶媒体駆動装置)とSCSIコントローラ27を介して接続してある。フロッピーディスク装置20はフロッピーディスクコントローラ19を介してバス2へ接続されている。

【0013】フロッピーディスク装置20には、フロッピーディスクが挿入され、このフロッピーディスク等やハードディスク装置13(またはMO、CD-ROM、DVD等の記憶媒体)、ROM14には、オペレーティングシステムと協働してCPU等に命令を与え、本発明を実施するためのコンピュータ・プログラムのコード若しくはデータを記録することができ、メモリ4にロードされることによって実行される。このコンピュータ・プログラムのコードは圧縮し、または、複数に分割して、複数の媒体に記録することもできる。

【0014】システム100は更に、ユーザ・インターフェース・ハードウェアを備え、入力をするためのポインティング・デバイス(マウス、ジョイスティック等)7またはキーボード6や、視覚データをユーザに提示するためのディスプレイ12を有することができる。また、パラレルポート16を介してプリンタを接続することや、シリアルポート15を介してモデムを接続することが可能である。このシステム100は、シリアルポート15およびモデムまたは通信アダプタ18(イーサネットやトークンリング・カード)等を介してネットワーク(インターネット)に接続し、暗号鍵を送信したり、他のコンピュータ等と通信を行うことが可能である。またシリアルポート15若しくはパラレルポート16に、遠隔送受信機器を接続して、赤外線若しくは電波によりデータの送受信(例えば受信者への暗号鍵の送信など)を行うことができる。

【0015】スピーカ23は、オーディオ・コントローラ21によってD/A(デジタル/アナログ変換)変換された音声信号を、アンプ22を介して受領し、音声として出力する。また、オーディオ・コントローラ21は、マイクロフォン24から受領した音声情報をA/D(アナログ/デジタル)変換し、システム外部の音声情報をシステムにとり込むことを可能にしている。

【0016】このように、本発明の暗号鍵生成システム及び暗号鍵配信システムは、通常のパーソナルコンピュータ(PC)やワークステーション、ノートブックP

C、パームトップPC、ネットワークコンピュータ、コンピュータを内蔵したテレビ等の各種家電製品、通信機能を有するゲーム機、電話、FAX、携帯電話、PHS、電子手帳、等を含む通信機能有する通信端末、または、これらの組合せによって実施可能であることを容易に理解できるであろう。ただし、これらの構成要素は例示であり、その全ての構成要素が本発明の必須の構成要素となるわけではない。

【0017】図5に鍵の具体的な変更の方法を示す。例えばアリスがあるとき視聴料を支払って、正当な受信者となったと仮定する。サーバーは、アリスに鍵K7を割り当て、アリスの公開鍵で暗号化して送る。また、K3をK7で暗号化したもの、すなわちK7(K3)、さらにK3(K1)、K1(K0)というように、ルートのセッション鍵に至る一連の鍵のチェーンをアリスに送る。受信者の全体数がnである場合、アリスのキーチェーンの大きさは $\log(n)$ ほどである。ここで、キャロルが何らかの理由で視聴者の集合Sから脱退した場合を考える。キャロルは、彼女のキーチェーンに、K0、K1、K4、K10という鍵を持っている。したがって、今後キャロルにコンテンツをアクセスさせないためには、これらの鍵を再発行して、キャロルの鍵を無効にしなければならない(図5の、Xのついている鍵である)。

【0018】K1を再発行してK1'としたとする。すると、アリスは自分の持っているK1が無効になってしまうので、新しいK1'をK3で暗号化したK3(K1')を受け取る必要がある。同様に、K0'は、K1'(K0')とK2(K0')という二つの鍵配送パッケージで受信者に知らせる必要がある。これにより、アリスはK1'とK0'を知ることになり、次から新しいセッション鍵K0'で暗号化されるコンテンツを見ることができる。このように、本発明の階層的鍵構造により、複数の受信者の中から、脱退者がした場合、脱退者が有する暗号鍵に関連する鍵のみを変更して、変更された鍵に対応する受信者にのみ、変更された暗号鍵を、その鍵の直下の鍵で暗号化して、配信することができるので、暗号鍵更新のための手間を最小にすることができる。

【0019】次に鍵の再配送効率については以下のようになる。例えばキャロルが脱退したときの、鍵の再配送に必要なパッケージ数を計算する。キャロルが持っていた鍵は $\log_2(n)$ 個であるから、新しく生成しなければならない鍵の数も $\log_2(n)$ である(厳密にいうと上の方式では $\log_2(n)$ より1小さい)。新しい鍵1個について、その鍵を、その2つの子供の鍵で暗号化して送る必要がある。従って、鍵の再配送に必要な鍵配送パッケージの数は、 $2 * \log_2(n)$ である。一般にr進木の場合を考えると、鍵再配送パッケージの数pは

$$p = r * \log_2(n)$$

$$= r * \log(n) / \log(r)$$

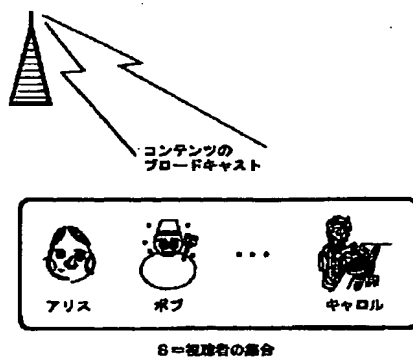
となる。nが一定の時、pを最小にするrは、 $r=e$ である(e

は自然対数の底)が、実際には r は自然数であるので、 $r=3$ の時が最適となり、パケット数はおよそ $2.73 \cdot \log(n)$ となる。また $r=2$ の場合と $r=4$ の場合では理論上パケットの数は同じであるので、2進木を使用するのであれば4進木を使用した方が現実的には有利であろう。

【0020】例えば、 n が100万、すなわち、100万人の視聴者にコンテンツを放送していると仮定する。ある一人の視聴者を外すためには、2進木の場合 $2 \cdot \log_2(106)$ 個すなわち、40個の鍵再配送パケットを放送すればよい。3進木の場合は $2.73 \cdot \log(106)=37.7$ であるので、鍵の暗号化方式としてDESを用いるとすれば、一つの鍵を64ビット+鍵のIDで送れるので、鍵のIDを32ビットとしても、鍵配送パケットのペイロードは96ビット(12バイト)であり、これが38個で全体が0.5Kバイトに収まる。

【0021】次に複数の脱退をまとめて計算する方法を以下に示す。もし、 k 人がまとめて脱退した場合、 $k \cdot \log(n)$ 個の鍵を新たに生成する必要はない。例えば、 K_0 は1回だけ更新すればよいからである。また、何人かが同時期に脱退することがあらかじめわかっている場合(月末までの契約で視聴している場合、など)は、それらの視聴者をできるだけ同じ枝(グループ)にまとめることで、複数の脱退が起きたときの鍵の更新と再配送を小さくすることができる。すなわち、複数の受信者を、予め受信者の属性によりグループ分けを行い、グループ間の関係に従い、複数の受信者を、木構造の形に階層的に配置された鍵と対応付けておけば、非常に効率的な、鍵の生成及び配信を行うことができる。また、受信者の属性として、契約年数、加入時期、年齢、職業、住所、会*

【図1】



* 社、電話番号、その他個人的な情報などを用いてもよい。本発明の本質に拘らず適宜変更可能である。

【0022】

【発明の効果】本発明により、既知の暗号技術の上で動くために規格を公開でき、各社の相互接続性が保たれ、また、上り回線を使うことなく、ダイナミックに特定の視聴者を参加させたり脱退させたりすることのできる、効率的な暗号鍵の配信が可能となる。また、配信途中にいくらセキュリティ上の問題がある経路があっても全体のセキュリティを保つことができる。

【0023】

【図面の簡単な説明】

【図1】衛星放送によりコンテンツのブロードキャストを行う概要図である。

【図2】従来のメイリングリストの暗号化の標準化案の概要を示す図である。

【図3】従来の Join/Leave Model の概要を示す図である。

【図4】本発明の暗号鍵配信のための鍵の階層構造の例を示す図である。

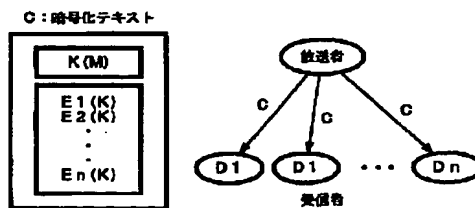
【図5】本発明の、ユーザの脱退による鍵の変更例を示す図である。

【図6】本発明の、暗号鍵生成システムのブロック図である。

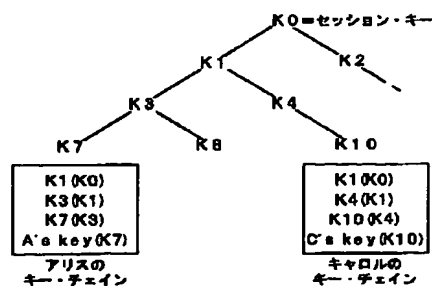
【図7】本発明の、暗号鍵配信システムのブロック図である。

【図8】本発明の暗号鍵配信システムのハードウェア構成の一実施例を示す図である。

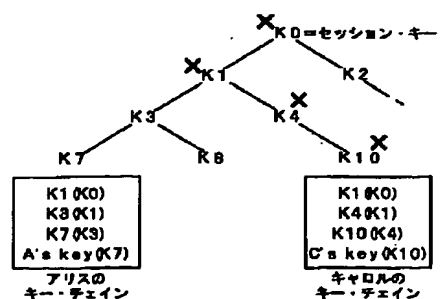
【図2】



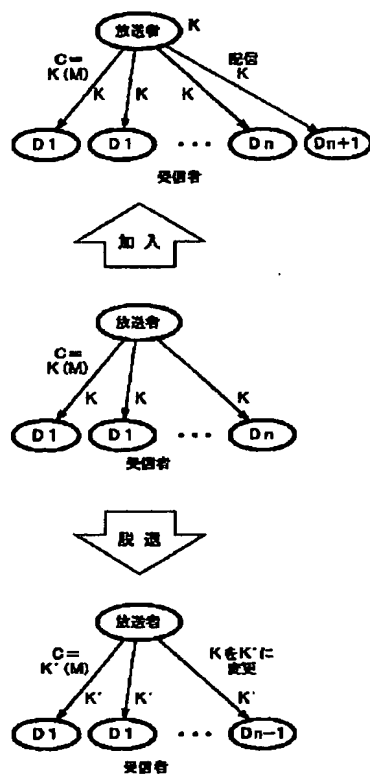
【図4】



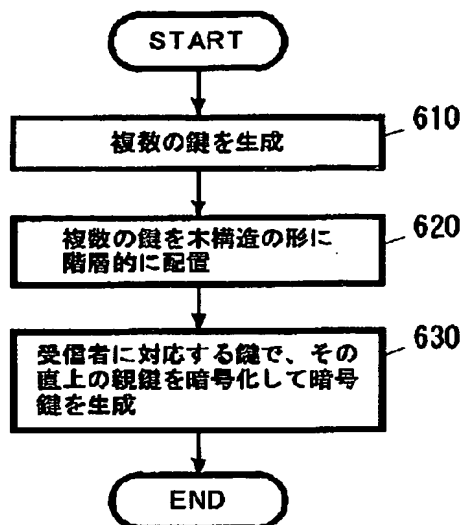
【図5】



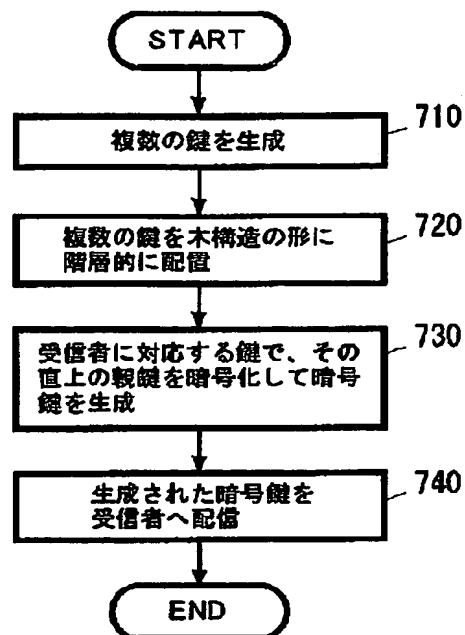
【図3】



【図6】



【図7】



【図8】

